

Serial No. 09/966,890
Preliminary Amendment and Response to Final Office Action
Mailed: 16-May-2008

REMARKS

This reply is in response to the Final Office Action dated 16-May-2008. In the Final Office Action Examiner rejected claims 1, 3-6, 9-11, 13-19, 22-27, 29-38, and 41. Claims 13-18, 27, 29-32, 35, and 41 remain pending in this application. By this paper, the Applicants hereby cancel claims 1-12, 19-26, 28, 33-34, and 36-40. Also, claims 13 and 27 have been amended to clarify and emphasize a primary objective of the invention, and to expedite allowance of the present application. Lastly, in light of the amendments and primary focus of remaining claims the Applicant has also requested to amend the title. These amendments do not add new matter. In view of the foregoing amendments and the following remarks, Applicants respectfully request consideration and allowance of all pending claims.

Rejections under 35 U.S.C. § 102

The Examiner rejected claims 13-18, 27, 29-32, 35, and 41 under 35 U.S.C. § 102(e) as being anticipated by Application Publication No. 20020172359 A1 to Markku-Juhani Saarinen, hereinafter referred to as Saarinen. Applicants respectfully traverse these rejections.

Legal Precedent

For a prior art reference to anticipate in terms of 35 U.S.C. § 102, every element of the claimed invention must be identically shown in a single reference. *Diversitech Corp. v. Century Steps, Inc.*, 850 F.2d 675, 677 (Fed. Cir. 1988). Thus, a claim is anticipated under 35 U.S.C. §

Serial No. 09/966,890
Preliminary Amendment and Response to Final Office Action
Mailed: 16-May-2008

102 if each and every limitation is found either expressly or inherently in a single prior art reference. *IPXL Holdings, L.L.C. v. Amazon.com, Inc.*, 430 F.3d 1377, 1381 (Fed. Cir. 2005). Following the above logic, an applicant need only show that a single element is not found in the cited reference in order to demonstrate that the cited reference does not anticipate the applicant's claimed subject matter.

The Saarinen Reference is missing at least one element in claims 13-18, 27, 29-32, 35, and 41

Applicants respectfully assert that Saarinen does not anticipate 13-18, 27, 29-32, 35, and 41 under 35 U.S.C. § 102, because not every element of the claimed invention is disclosed. *See id.* Specifically, the Applicant discloses, in independent claim 13, 27, and 41, an embodiment that uses a signature value which is a known fixed value that makes up only a portion of the seed pool. Additionally, the Applicant's signature value can change upon a triggering event, and does not change randomly between re-seeding of the seed pool. The Applicant's signature value can change based on a masking of the least significant bit of a timer into the seed pool, at a location in the seed pool determined by a pointer. The masking of the least significant bit will occur upon the detection of a triggering event such as a main power cycle or reboot. Lastly, the signature value is tracked and evaluated to determine the amount of change that has occurred to it. The tracking and evaluation of the signature value provides for the ability to bypass the cryptographic security subsystem up until a predetermined threshold amount of change in the signature value is reached. As a result, if the cryptographic security subsystem is in "bypass mode" then a

Serial No. 09/966,890
Preliminary Amendment and Response to Final Office Action
Mailed: 16-May-2008

technician or user, for a period of time, can still access the processor-based device without having to undergo a time consuming process of establishing a secure session.

Contrary to the Examiner's argument, there are no claims in Saarinen which explicitly disclose the use of a signature value as a means of bypassing a cryptographic security subsystem to allow access to a processor-based device for a period of time. Thus, independent claims 13, 27, 41 should be allowed, as well as dependent claims 14-18, 29-32, and 35. Firstly, the Examiner argues that Saarinen, paragraph 76, allegedly discloses a signature value by equating the counter variable and constant used in Saarinen to the Applicant's disclosed signature value. Office Action, page 3. Specifically, the Examiner provides an explanation for equating Saarinen's counter variable and constant to the Applicant's signature value merely stating that, the counter variable and constant "are set but altered with the seeding of the pool to make it more difficult for attackers to gain access to the system." *See id.* The counter variable referred to by the Examiner, in Saarinen paragraph 76, is a random variable which changes randomly between re-seeding and is incremented by a constant.

Accordingly, the purpose of the counter variable and constant disclosed in Saarinen is to populate the seed pool in a way that increases entropy, thus making it more difficult for unauthorized access to the system. In addition, the Examiner argues that Saarinen discloses the enabling and disabling of a secure communication session. *See* Office Action at page 4-5. In light of the Examiner's arguments, the Examiner incorrectly suggests that the primary and sole purpose of the Applicant's signature value is to increase entropy and make it more difficult for unauthorized access to the system. However, unlike Saarinen, a purpose of the Applicant's

Serial No. 09/966,890
Preliminary Amendment and Response to Final Office Action
Mailed: 16-May-2008

signature value is not merely to increase entropy and disable and enable the cryptographic security subsystem, but also to allow access to the processor-based device by bypassing the cryptographic security subsystem up to a predetermined threshold amount of change in the signature value. The bypass allows for the ability to still access the processor-based device despite the presence of the cryptographic security subsystem. Hence, in the Applicant's disclosure of the signature value, a primary focus is placed on bypassing the cryptographic security subsystem for a period of time to allow access to the processor-based device. The primary focus of this application is not on achieving entropy through the signature value. Even if the counter variable and constant disclosed in Saarinen are interpreted to be a signature value, there is no clear indication in the claims or specification of Saarinen that the counter variable and constant are being processed, tracked, or evaluated in order to determine the amount of change that has occurred to the counter variable and constant. For the above reasons, the counter variable and constant disclosed in Saarinen do not anticipate the claims associated with the Applicant's disclosed signature value. *See Diversitech*, 850 F.2d at 677.

Lastly, the Examiner argues that paragraph 55 provides additional support for the 35 U.S.C. § 102(e) claim rejections, wherein paragraph 55 describes a random number generation process for generating a random number without using a new input seed. *See Office Action* at page 4. The said generation process begins by adding a constant C to the current randomly generated counter variable T and placing the result in the output buffer as the new input seed. Afterwards, the said input seed remains unchanged, and it may be used to generate subsequent random numbers. However, the Applicant's signature value is distinguished from the counter

Serial No. 09/966,890
Preliminary Amendment and Response to Final Office Action
Mailed: 16-May-2008

variable and constant disclosed in Saarinen, because the Applicant's signature value makes up only a portion of the input seed. In addition, the Applicant's signature value, within the input seed, can change based on a masking of the least significant bit of a timer into the input seed at a location in memory indicated by an incremented pointer. On the other hand, the counter variable and constant referred to in Saarinen, paragraph 55 and further elaborated on in paragraph 56, makes up the total input seed and the input seed does not change. Hence, Saarinen does not anticipate the claims relating to the Applicant's disclosed signature value. *See Diversitech*, 850 F.2d at 677.

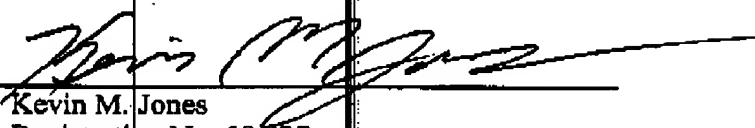
Serial No. 09/966,890
Preliminary Amendment and Response to Final Office Action
Mailed: 16-May-2008

Conclusion

The Applicant respectfully submits that all pending claims are in condition for allowance. However, if the Examiner wishes to resolve any other issues by way of a telephone conference, the Examiner is kindly invited to contact the undersigned at the telephone number indicated below.

Respectfully submitted,

Date: 16 July 2008


Kevin M. Jones
Registration No. 58,827
(281) 514-7828

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
Legal Department, M/S 35
P.O. Box 272400
Fort Collins, Colorado 80527-2400